

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Emmanuel Prouff (Ed.)

Smart Card Research and Advanced Applications

10th IFIP WG 8.8/11.2 International Conference
CARDIS 2011

Leuven, Belgium, September 14-16, 2011

Revised Selected Papers

Volume Editor

Emmanuel Prouff
Oberthur Technologies
71-73 rue des Hautes Pâtures
92726 Nanterre Cedex, France
E-mail: e.prouff@oberthur.com

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-27256-1 e-ISBN 978-3-642-27257-8
DOI 10.1007/978-3-642-27257-8
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011943215

CR Subject Classification (1998): E.3, C.2, K.6.5, D.4.6, C.3, D.2

LNCS Sublibrary: SL 4 – Security and Cryptology

© IFIP International Federation for Information Processing 2011
This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.
The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

These proceedings contain the papers selected for CARDIS 2011, the 10th IFIP Conference on Smart Card Research and Advanced Applications hosted by the Katholieke Universiteit of Leuven, Belgium. Since 1994, CARDIS has been the foremost international conference dedicated to the security of smart cards and embedded systems. Initially biennial, the conference became annual in 2010 to take into account the very fast evolution of the smart card technology.

Security of smart cards is today an established and dynamic research area. Since 1994, CARDIS offers a privileged environment where the scientific community can congregate, present new ideas and discuss recent developments with both an academic and industrial focus. It covers a wide range of topics including hardware design, operating systems, systems modelling, cryptography and systems security. This year, the Program Committee of CARDIS refereed 45 submitted papers. Each paper was reviewed by at least 3 referees and the committee selected 20 papers to be presented at the conference. Two invited talks completed the technical program. The first one was given by Helena Handschuh, Chief Technology Officer at Intrinsic-ID, and the second one, by Olivier Ly, Associate Professor at LaBRI, University of Bordeaux.

There are many volunteers who offered time and energy to put together the symposium and who deserve our acknowledgement. I first would like to thank all the members of the Program Committee and the external reviewers for their hard work in evaluating and discussing the submissions. I am also very grateful to Vincent Rijmen, the General Chair of CARDIS 2011, and his team for the local conference management. I am particularly grateful to the CARDIS Steering Committee for allowing me to serve at such a recognized conference. Especially, I would like to say a big thank you to Jean-Jacques Quisquater for all the energy and hard work he put into the organization of this event.

Last, but certainly not least, my thanks go to all the authors who submitted papers and all the attendees. I hope you will find the proceedings stimulating.

September 2011

Emmanuel Prouff

Sergei Skorobogatov
François-Xavier Standaert
Pim Tuyls
David Vigilant

University of Cambridge, UK
UCL Crypto Group, Belgium
Intrinsic-ID, The Netherlands
Gemalto, France

Referees

J. Balasch
S. Riou
A. Barenghi
M. Rousset
E. Beck
S. Salgado
A. Berzati
G. Schrijen
S. Bhasin
M. Seysen
B. Brumley
J. Soria-Comas
C. Capel
A. Séré
C. Clavier
P. Teuwen
I. Coisel
C. Troncoso

J. Daemen
R. Trujillo-Rasua
E. De Mulder
G. Van Assche
F. De Santis
V. Van Der Leest
E. Dottax
N. Veyrat-Charvillon
I. Eichhorn
K. Villegas
J. Fan
O. Farràs
W. Fischer
G. Gagnerot
B.M. Gammel
J. Großschädl
V. Guérin
S. Hajian

L. Hoffmann
M. Hutter
M. Kasper
C.H. Kim
S.-K. Kim
F. Koeune
S. Kutzner
M. Le Guin
M. Medwed
F. Melzani
O. Mischke
D. Oswald
P. Paillier
T. Plos
B. Qin
M. Quisquater
F. Regazzoni

Sponsoring Institution

Oberthur Technologies

Table of Contents

Smart Cards System Security

Evaluation of the Ability to Transform SIM Applications into Hostile Applications.....	1
<i>Guillaume Bouffard, Jean-Louis Lanet, Jean-Baptiste Machemie, Jean-Yves Poichotte, and Jean-Philippe Wary</i>	
Synchronized Attacks on Multithreaded Systems - Application to Java Card 3.0	18
<i>Guillaume Barbu and Hugues Thiebauld</i>	
A Formal Security Model of a Smart Card Web Server.....	34
<i>Pierre Neron and Quang-Huy Nguyen</i>	

Invasive Attacks

Differential Fault Analysis of AES-128 Key Schedule Using a Single Multi-byte Fault	50
<i>Sk Subidh Ali and Debdeep Mukhopadhyay</i>	
Combined Fault and Side-Channel Attack on Protected Implementations of AES	65
<i>Thomas Roche, Victor Lomné, and Karim Khalfallah</i>	
Memory-Efficient Fault Countermeasures.....	84
<i>Marc Joye and Mohamed Karroumi</i>	

New Algorithms and Protocols

Redundant Modular Reduction Algorithms	102
<i>Vincent Dupaquis and Alexandre Venelli</i>	
Fresh Re-keying II: Securing Multiple Parties against Side-Channel and Fault Attacks.....	115
<i>Marcel Medwed, Christoph Petit, Francesco Regazzoni, Mathieu Renauld, and François-Xavier Standaert</i>	

Fast Key Recovery Attack on ARMADILLO1 and Variants 133
Pouyan Sepehrdad, Petr Sušil, and Serge Vaudenay

Implementations and Hardware Security 1

Implementation and Evaluation of an SCA-Resistant Embedded
 Processor 151
Stefan Tillich, Mario Kirschbaum, and Alexander Szekely

Evaluating 16-Bit Processors for Elliptic Curve Cryptography 166
Erich Wenger and Mario Werner

A Hardware Processor Supporting Elliptic Curve Cryptography for
 Less than 9kGEs 182
Erich Wenger and Michael Hutter

Implementations and Hardware Security 2

Memory Encryption for Smart Cards 199
Bariş Ege, Elif Bilge Kavun, and Tolga Yalçın

Compact FPGA Implementations of the Five SHA-3 Finalists 217
*Stéphanie Kerckhof, François Durvaux, Nicolas Veyrat-Charvillon,
 Francesco Regazzoni, Gueric Meurice de Dormale, and
 François-Xavier Standaert*

Non-invasive Attacks

An Exploration of the Kolmogorov-Smirnov Test as a Competitor to
 Mutual Information Analysis 234
Carolyn Whitnall, Elisabeth Oswald, and Luke Mather

A High-Performance Implementation of Differential Power Analysis on
 Graphics Cards 252
Timo Bartkewitz and Kerstin Lemke-Rust

RAM: Rapid Alignment Method 266
Ruben A. Muijrrers, Jasper G.J. van Woudenberg, and Lejla Batina

Java Card Security

Combined Software and Hardware Attacks on the Java Card
 Control Flow 283
Guillaume Bouffard, Julien Iguchi-Cartigny, and Jean-Louis Lanet

Java Card Operand Stack: Fault Attacks, Combined Attacks and Countermeasures.....	297
<i>Guillaume Barbu, Guillaume Duc, and Philippe Hoogvorst</i>	
Formal Analysis of CWA 14890-1	314
<i>Ashar Javed</i>	
Author Index	337